



Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at <http://about.jstor.org/participate-jstor/individuals/early-journal-content>.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

REPRESENTATIONS OF THE GENERAL SYMMETRIC GROUP AS LINEAR GROUPS IN FINITE AND INFINITE FIELDS*

BY

LEONARD EUGENE DICKSON

1. In a series of articles in the *Berliner Berichte*, beginning in 1896, FROBENIUS has developed an elaborate theory of group-characters and applied it to the representation of a given finite group G as a non-modular linear group. Later, BURNSIDE † approached the subject from the standpoint of continuous groups. The writer has shown ‡ that the method employed by BURNSIDE may be replaced by one involving only purely rational processes and hence leading to results valid for a general field. The last treatment, however, expressly excludes the case in which the field has a modulus which divides the order of G . The exclusion of this case is not merely a matter of convenience, nor merely a limitation due to the particular method of treatment; indeed, § the properties of the group-determinant differ essentially from those holding when the modulus does not divide the order of G . || Thus when G is of order $q!$, the general theory gives no information as to the representations in a field having a modulus $\leq q$, whereas the case of a small modulus is the most important one for the applications.

The present paper investigates the linear homogeneous groups on m variables, with coefficients in a field F , which are simply isomorphic with the symmetric group on q letters. The treatment is elementary and entirely independent of the papers cited above; in particular, the investigation is made for all moduli without exception. The principal result is the determination of the minimum value of the number of variables. It is shown that $m \geq q - 1$ or $m \geq q - 2$, according as F has not or has a modulus p which divides q (§§ 8–21). There

* Presented to the Society (Chicago), March 30, 1907. Received for publication April 17, 1907.

† Proceedings of the London Mathematical Society, vol. 29 (1898), pp. 207–224, 546–565; vol. 35 (1902), pp. 206–220.

‡ These Transactions, vol. 3 (1902), pp. 285–301.

§ DICKSON, Proceedings of the London Mathematical Society, vol. 35 (1902), p. 68.

|| Since the present paper was written, the writer has obtained some general results on the outstanding case in which the modulus divides the order of G , these Transactions, vol. 8 (1907), pp. 389–398; Bulletin of the American Mathematical Society, vol. 13 (1907), pp. 477–488.

is a representation on $q - 1$ variables, except in the trivial case $q = p = 2$ (§ 2); while for any field having a modulus which divides there is a representation on $q - 2$ variables, except in the special cases $q \leq 4$ (§ 4).

The determination of the possible representations is made for a case considerably more general than the special one found to be sufficient in establishing the minimum value of m (cf. § 11). We thereby gain a better insight into the nature of the general problem. The question of the equivalence, under linear transformation, of the resulting linear groups is treated in §§ 22–24.

The most essential point in the proof leading to a minimum for m may be seen in a typical case in § 13. After the preliminary normalizations, the transformations involve two sets of parameters. With these we form two rectangular matrices A, B . Then the conditions on the parameters are equivalent to the condition that the product AB shall equal a known matrix M . The representation on m variables is thus possible if and only if the elements of the two matrices A and B can be determined in the field so that $AB = M$. The problem is thus reduced to a simple question of determinants.

2. The symmetric group $S_{q!}$ on q letters is isomorphic with the group of the transformations

$$(1) \quad x'_i = x_{a_i} \quad (a' \text{'s a permutation of } 1, \dots, q).$$

In place of x_q we introduce the new variable

$$(2) \quad \omega = x_1 + \dots + x_q,$$

and then suppress ω . According as $a_q = q$ or $a_t = q$ ($t < q$), we get

$$(3) \quad x'_i = x_{a_i} \quad (a' \text{'s a permutation of } 1, \dots, q-1),$$

$$(4) \quad x'_i = -\sum_{j=1}^{q-1} x_j, \quad x'_i = x_{a_i} \text{ [the } a_i \text{ (} i \neq t \text{) a permutation of } 1, \dots, q-1 \text{ with } a_q \text{ omitted].}$$

Except when $q = 2$ and the coefficients are taken modulo 2, (4) is not the identity I , and the isomorphism is simple. Henceforth we shall take $q > 2$.

3. The transformations (1) leave invariant (2) and

$$(5) \quad \omega_2 = \sum x_i x_j, \quad \omega_3 = \sum x_i x_j x_k \quad (i, j, k = 1, \dots, q; i < j < k \dots).$$

Eliminating x_q from ω_2 by means of (2), we get

$$\omega_2 = \omega \sum_{i=1}^{q-1} x_i - \phi_{q-1},$$

where

$$(6) \quad \phi_{q-1} = \sum x_i^2 + \sum x_i x_j \quad (i, j = 1, \dots, q-1; i < j).$$

Hence ϕ is an invariant (in fact, the only quadratic invariant) of the group of

the transformations (3), (4). For the new variables

$$(7) \quad y_{q-1} = x_{q-1}, \quad y_i = x_i - x_{q-1} \quad (i = 1, \dots, q-2),$$

we have

$$(8) \quad \phi_{q-1}(x) = \phi_{q-2}(y) + qy_{q-1} \sum_{i=1}^{q-2} y_i + \frac{1}{2}q(q-1)y_{q-1}^2.$$

We assume that the coefficients of our transformations and invariants may be reduced modulo p , where p is any fixed divisor of q . If p is odd, or if both p and q/p are even, the second member of (8) reduces to $\phi_{q-2}(y)$. The possibility of this reduction of the number of variables follows directly from the fact that the discriminant of (6) equals q .

4. We next discuss the nature of transformations (3), (4), when expressed on the variables (7). We show that if the coefficients be reduced modulo p , a divisor of q , then $y'_k (k < q-1)$ is a linear function of y_1, \dots, y_{q-2} . Now $y'_k = x'_k - x'_{q-1}$. For (3), this equals $x_{\alpha_k} - x_{\alpha_{q-1}}$ and hence, by (7), equals a function of the $y_i (i < q-1)$. A like result holds for (4) if k and $q-1$ are both distinct from t . If $k = t$ or if $q-1 = t$, y'_k involves q x 's with like sign and hence equals a function of the y 's in which the coefficient of y_{q-1} is $\pm q$. Hence $S_{q!}$ is simply or multiply isomorphic with a linear homogeneous group $L_{q-2, p}$ on $q-2$ variables modulo p . The substitutions of S which correspond to the identity in L form an invariant subgroup J of S . For $q > 4$, J is the identity or else it contains all even substitutions on the q letters. But for $q > 4$, $[x_1 x_2 x_3] \sim [y_1 y_2 y_3]$, so that the isomorphism is simple. For $q = 3$,

$$[x_1 x_2 x_3] \sim I, \quad [x_1 x_2] \sim y'_1 = -y_1,$$

so that $L_{1,3}$ is of order 2, and the isomorphism is (3, 1). For $q = 4$,

$$\begin{aligned} [x_1 x_3] [x_2 x_4] &\sim y'_1 = -y_1, & y'_2 &= -2y_1 - y_2; \\ [x_1 x_4] [x_2 x_3] &\sim y'_1 = -y_1 - 2y_2, & y'_2 &= -y_2; \\ [x_1 x_2] &\sim [y_1 y_2], & [x_1 x_3] &\sim y'_1 = -y_1, & y'_2 &= -y_1 + y_2. \end{aligned}$$

Hence $S_{4!}$ is simply isomorphic with $L_{2,4}$, but has (4, 1) isomorphism with $L_{2,2}$. Moreover, $S_{4!}$ cannot be represented as a binary group in a finite or infinite field having modulus 2. Indeed, the transformations of period 2 are conjugate with $(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix})$, which is commutative only with $(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix})$. The square of the latter is $(\begin{smallmatrix} a^2 & 0 \\ 0 & a^2 \end{smallmatrix})$. But $a^4 = 1$ requires $a = 1$ in any field with modulus 2. Hence there is no binary transformation of period 4 commutative with $(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix})$, whereas $S_{4!}$ has a cyclic subgroup of order 4.

THEOREM. *For $q > 4$, the symmetric group on q letters is simply isomorphic with a linear homogeneous group on $q-2$ variables with integral coefficients taken modulo p , where p is any integral divisor > 1 of q . For*

$q = 4$, the result holds if $p = 4$, but not if $p = 2$. The case $q = 3$ is exceptional since a unary homogeneous group is commutative.

5.* If p is an odd prime dividing q , the group $L_{q-2,p}$ has (§ 3) the invariant $\phi_{q-2}(y)$ of discriminant $q - 1 \equiv -1 \pmod{p}$. Hence the invariant can be reduced by a linear transformation with integral coefficients to

$$(9) \quad Y_\epsilon \equiv y_1^2 + \cdots + y_{q-3}^2 + \epsilon y_{q-2}^2, \quad \left(\frac{\epsilon}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right)^{q-2}.$$

According as ϵ is a square or a not-square in a field F , the group defined by the invariant Y_ϵ is called a first or a second orthogonal group in F . In particular, for the $GF[p^n]$ the group is a first or second orthogonal group according as

$$(10) \quad \left(\frac{-1}{p}\right)^n \left(\frac{2}{p}\right)^{n(q-2)} = +1 \text{ or } -1.$$

Next let $p = 2$. The quadratic form

$$(11) \quad Q_{2m} = \sum \xi_i^2 + \sum \xi_i \xi_j \quad (i, j = 1, \dots, 2m; i < j)$$

can be reduced by a linear transformation with integral coefficients to

$$(12) \quad f_c = \xi_1 \xi_2 + \cdots + \xi_{2m-1} \xi_{2m} + c(\xi_1^2 + \xi_2^2),$$

where $c \equiv 0$ or $1 \pmod{2}$ according as 2 is a quadratic residue or non-residue of the discriminant $2m + 1$ of Q_{2m} . For the $GF[2^n]$, f_1 can be reduced to f_0 if and only if n be even. The group defined by the invariant f_0 is called the first hypoabelian group; that defined by f_1 with $\xi_1 \xi_2 + \xi_1^2 + \xi_2^2$ irreducible is called the second hypoabelian group. Hence the group defined by the invariant Q_{2m} in the $GF[2^n]$ can be transformed into the first or second hypoabelian group according as

$$(13) \quad \left(\frac{2}{2m+1}\right)^n = +1 \text{ or } -1.$$

Next, $\xi_0^2 + Q_{2m}$ can be reduced to $\xi_0^2 + f_0$, since the operation

$$\xi'_0 = \xi_0 + \xi_1 + \xi_2, \quad \xi'_i = \xi_i \quad (i > 0)$$

replaces $\xi_0^2 + f_c$ by $\xi_0^2 + f_{c+1}$. Now for $p = 2$, $q/2$ odd, the analysis in § 3 failed to exhibit a quadratic invariant for the group on y_1, \dots, y_{q-2} , but led to the invariant $\phi_{q-2}(y) + y_{q-1}^2$ for the group on y_1, \dots, y_{q-1} . Hence the latter group can be transformed into one with the invariant

$$y_1 y_2 + y_3 y_4 + \cdots + y_{q-3} y_{q-2} + y_{q-1}^2.$$

* The results of §§ 5, 6, are not employed in the subsequent sections.

By an elementary discussion (the writer's *Linear Groups*, p. 200), the group is seen to be simply isomorphic with an abelian linear group on $q - 2$ variables. An independent proof follows from § 6.

THEOREM. *There exist representations of the symmetric group on q letters as linear homogeneous groups as follows:*

- (i) *for q odd, a first or second hypoabelian group in the $GF[2^n]$ on $q - 1$ variables, according as $(2/q)^n = +1$ or -1 ;*
- (ii) *for $q = 4l > 4$, a first or second hypoabelian group in the $GF[2^n]$ on $q - 2$ variables, according as $[2/(q - 1)]^n = +1$ or -1 ;*
- (iii) *for $q = 4l + 2 > 2$, an abelian linear group in any field F_2 having modulus 2 on $q - 2$ variables.*

By considering the monodromy group of the equation for the bisection of the periods of certain abelian functions, JORDAN has shown (*Traité des Substitutions*, p. 364, § 498) that the symmetric group on q letters is simply isomorphic with an abelian linear group modulo 2 on $2k$ variables, k being the greatest integer in $\frac{1}{2}(q - 1)$. The exceptional character of the case $q = 4$ was overlooked. The theorem obtained above shows that if $q \neq 4l + 2$ the abelian group may be taken to be a hypoabelian group.

Additional properties of our linear groups may be obtained by employing the further invariants * (5). Proceeding with ω_3 and ω_4 as we did with ω_2 in § 3, we obtain functions independent of y_{q-1} if and only if $p = 2$ and $p = 3$, respectively. Thus for $p = 2, 3$, the group $L_{q-2,p}$ has the respective invariants

$$(14) \quad \sum y_j^2 y_k, \quad \sum y_j^2 y_k y_l \quad (j, k, l = 1, \dots, q - 2; j, k, l \text{ distinct}; k < l).$$

6. The fact that the symmetric group on $2k$ letters ($2k > 4$) is simply isomorphic with an abelian group modulo 2 on the variables ξ_i, η_i ($i = 1, \dots, k - 1$) may also be shown by the following correspondence of generators:

$$\begin{aligned} [12] &\sim L'_1, \quad [23] \sim L_1, \quad [34] \sim V_{12}, \quad [45] \sim L_2, \quad [56] \sim V_{23}, \quad \dots, \\ [2i, 2i + 1] &\sim L_i, \quad [2i + 1, 2i + 2] \sim V_{i+1}, \quad \dots, \\ [2k - 2, 2k - 1] &\sim L_{k-1}, \quad [2k - 1, 2k] \sim L'_{k-1}, \end{aligned}$$

in which the L 's and V 's alternate. Here

$$\begin{aligned} L_i: \xi'_i &= \xi_i + \eta_i; & L'_i: \eta'_i &= \eta_i + \xi_i; \\ V_{ij} \equiv V_{ji}: \eta'_i &= \eta_i + \xi_i + \xi_j, & \eta'_j &= \eta_j + \xi_i + \xi_j. \end{aligned}$$

Since each transformation is of period 2, and V_{ij} is commutative with L'_i, L'_j, V_{jk} , while $L'_i L_i$ and $L_i V_{ij}$ are of period 3, the above transformations satisfy

* If we assume that the variables, as well as the coefficients, are integers taken modulo 2, then the group $L_{q-2,2}$ has, for $q = 8t + 2$, the invariant

$$\sum y_j y_k y_l + \sum y_i y_j y_k y_l \quad (i, j, k, l = 1, \dots, q - 2; i < j < k < l)$$

MOORE's set* of generational relations for the abstract form of the symmetric group. If we transform by $L_1 L_2 \cdots L_{k-1}$, we obtain the generators

$$M_1, L_1, W_{12}, L_2, W_{23}, L_3, \dots, L_{k-1}, M_{k-1},$$

and hence have a direct generalization of the result for $k = 6$ in *Linear Groups*, §118, page 99. Here $W_{12} = S$.

For $k = 4$, the group generated by L'_1, L_1, \dots has the (single) quadratic invariant †

$$\xi_1 \eta_1 + \xi_2 \eta_2 + \xi_3 \eta_3 + \xi_1 + \xi_2 + \xi_3 + \eta_1 + \eta_3.$$

The abelian transformation $L'_2 L'_1 L_3 Q_{13}$ replaces this by

$$\xi_1 \eta_1 + \xi_2 \eta_2 + \xi_3 \eta_3.$$

Hence (in accord with §5) S_8 is representable as a first hypoabelian group. But the total first hypoabelian group modulo 2 on 6 variables is of order 8!.

THEOREM. ‡ The symmetric group on 8 letters is simply isomorphic with the total first hypoabelian group modulo 2 on 6 variables.

7. LEMMA. If the direct product of two groups A and B contains a subgroup G simply isomorphic with the symmetric group on n letters, then A or B contains a subgroup of that type.

Let the operations of G be $a_1 b_1, a_2 b_2, \dots$. Then the distinct a 's form a group α , the distinct b 's a group β . The largest group α' common to α and G is evidently invariant in each; the largest group β' common to β and G is invariant in each. As well known, the quotient-groups

$$\frac{G}{\{\alpha', \beta'\}}, \quad \frac{\alpha}{\alpha'}, \quad \frac{\beta}{\beta'}$$

are simply isomorphic. By hypothesis, G is simply isomorphic with S_ν , $\nu = n!$. Hence the only invariant subgroups of G_ν are itself, the identity I , the group $G_{\frac{1}{2}\nu}$ of the alternating type, and for $n = 4$ a "four group" G_4 . The lemma is obvious if either α' or β' is G itself, or if each is I , or if each is $G_{\frac{1}{2}\nu}$ (whence $n = 2$). Next let $\alpha' = G_{\frac{1}{2}\nu}$, $\beta' = I$. Then G is composed of the operations of $\alpha' = G_{\frac{1}{2}\nu}$ and the products of $\frac{1}{2}\nu$ further a 's by an operation b of period 2, so that G is simply isomorphic with α . Finally, if $n = 4$, and $\alpha' = G_4$, then β' cannot be of type G_4 or $G_{\frac{1}{2}\nu}$, so that $\beta' = I$; hence α is of order 4! and is simply isomorphic with G .

* Proceedings of the London Mathematical Society, vol. 28 (1896), p. 357. For $k > 2$ the isomorphism is simple in view of his theorem C.

† For $k = 5$, this abelian group on 8 variables has no linear or quadratic invariant. The subgroup corresponding to the alternating group on 1, \dots , 10 has no quadratic invariant.

‡ For a proof based on other principles, see the writer's note in the Bulletin of the American Mathematical Society, vol. 13, (1907), pp. 386-389.

8. THEOREM. *For q odd, the symmetric group on q letters cannot be represented as a linear homogeneous group on $q - 2$ variables with coefficients in a finite or infinite field F_2 having modulus 2.*

It follows from the theory of canonical forms that every transformation of period 2 of the general linear homogeneous group H on $q - 2$ variables in F_2 is conjugate within H with one of the transformations

$$(15) \quad \xi'_i = \xi_i, \quad \xi'_{r+i} = \xi_{r+i} + \xi_i, \quad \xi'_j = \xi_j \quad (i=1, \dots, r; j=2r+1, \dots, q-2),$$

where r is an integer such that $2r \leq q - 2$, whence $r \leq \frac{1}{2}(q - 3)$. The matrix of (15) and the matrix of the general transformation of H commutative with (15) may be given the compact notations

$$(16) \quad \begin{array}{cccccc} I & O & O & A & O & O \\ I & I & O, & C & A & D, \\ O & O & I & E & O & B \end{array}$$

in which each I is a unit or identity matrix, each O a matrix all of whose elements are zero, while A and B are square matrices of orders r and $q - 2 - 2r$, respectively.

Suppose now that H has a subgroup $G_{q!}$ of symmetric type. We may assume that the latter contains a transformation (15) corresponding to the transposition $[l_1 l_2]$, and that the group K of the transformations (16₂) contains a subgroup G_ω , $\omega = (q - 2)!$, simply isomorphic with the symmetric group on l_3, \dots, l_q . The group K has the invariant subgroup J ,

$$\begin{array}{cccccc} I & O & O & A & O & O \\ J: & C & I & D, & Q: & O & A & O, \\ E & O & I & O & O & B \end{array}$$

the quotient group K/J being simply isomorphic with Q . The largest group common to J and G_ω is invariant in the latter. Now every transformation of J is of order a power of 2. But, for $n \neq 4$, $S_{n!}$ contains no invariant subgroup of order a power of 2. Since q is odd, it follows that G_ω is simply isomorphic with a subgroup of Q , and hence (§ 7) with a subgroup of one of the linear groups A and B on r and $q - 2 - 2r$ variables, respectively. Since $1 \leq r \leq \frac{1}{2}(q - 3)$, we have $q - 2 - 2r \leq q - 4$, and, if $q \geq 5$, $r \leq q - 4$. Hence the theorem follows by induction from $q - 2$ to q , it being obviously true for $q = 3$, since a unary homogeneous group is commutative.

For q even, we apply the preceding theorem to the subgroup leaving l_q fixed and obtain the

COROLLARY. *For q even, $S_{q!}$ cannot be represented as a linear homogeneous group in F_2 on $q - 3$ variables.*

The preceding theorem and corollary form a sequel to the results of §§ 2, 4 for the case when the modulus is 2.

9. Henceforth we discuss the representations of $S_{q!}$ as an m -ary linear homogeneous group in a field F not having modulus 2. Within the general linear homogeneous group $GLH(m, F)$, any transformation of period 2 is conjugate with one of the form ΠC_i , where C_i alters only ξ_i , whose sign it changes. We thus assume that the transposition [12] corresponds to $C_1 C_2 \cdots C_r$. Then each transposition corresponds to a transformation (α_{ij}) with the characteristic determinant

$$(17) \quad |\alpha - \rho I| = (-1 - \rho)^r (1 - \rho)^{m-r}.$$

To [34] corresponds a transformation S commutative with $C_1 \cdots C_r$. Transforming $S = S_{1, \dots, r} S'_{r+1, \dots, m}$ by a transformation of type $T_{1, \dots, r} T'_{r+1, \dots, m}$, we obtain a product of r of the C_i . Hence*

$$(18) \quad [12] \sim C_1 \cdots C_r, \quad [34] \sim C_1 \cdots C_s C_{r+1} \cdots C_{2r-s} \quad (0 \leq s \leq r).$$

Since [13][24] is commutative with [12][34], we get

$$[13][24] \sim R S_{1, \dots, s, 2r-s+1, \dots, m}, \quad R = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

where α, \dots, δ are square matrices of order $r-s$, α affecting the variables ξ_{s+1}, \dots, ξ_r , and δ the variables $\xi_{r+1}, \dots, \xi_{2r-s}$. We may obtain [14][23] by transforming [13][24] by [12] or as the product [13][24] · [12][34]. Identifying the two results, we find that $\alpha = \delta = 0$, and that S is commutative with $C_1 \cdots C_r$. Also $\beta\gamma = \gamma\beta = I$, since $R^2 = I$. Hence

$$[13][24] \sim \begin{pmatrix} O & \beta \\ \beta^{-1} & O \end{pmatrix} \cdot S_{1, \dots, s} S'_{2r-s+1, \dots, m}.$$

We may take $\beta = I$, $S = C_1 \cdots C_s$, $S' = C_{2r-s+1} \cdots$, by transforming by

$$(\beta)_{r+1, \dots, 2r-s} T_{1, \dots, s} T'_{2r-s+1, \dots, m},$$

where T and T' are suitably chosen. Then (18) are unaltered, and

$$(19) \quad [13][24] \sim C_1 \cdots C_\sigma \prod_{i=1}^{r-s} (\xi_{s+i} \xi_{r+i}) \prod_{i=1}^{r-s-\sigma} C_{2r-s+i} \quad (0 \leq \sigma \leq s, \sigma \leq r-s).$$

The number of factors in the final product must be $r-s-\sigma$ since the number of roots -1 of the characteristic equation is $2r-2s$, [13][24] being conjugate with [12][34]. By (18) and (19), we have

$$(20) \quad [14][23] \sim C_1 \cdots C_\sigma \prod_{i=1}^{r-s} (\xi_{s+i} \xi_{r+i}) \prod_{i=s+1}^{3r-2s-\sigma} C_i.$$

* The terms $C_1 \cdots C_s$ are to be suppressed in the case $s=0$. Similarly below. For the case $q=3$, here excluded, we may proceed as in § 16, with $k=0$.

In applying (18) and (19) simultaneously, it is convenient to have the variables separated into the sets $\xi_{i_1}, \dots, \xi_{i_6}$, where

$$(21) \quad \begin{aligned} i_1 &= 1, \dots, \sigma; \quad i_2 = \sigma + 1, \dots, s; \quad i_3 = s + 1, \dots, r; \\ i_4 &= r + 1, \dots, 2r - s; \quad i_5 = 2r - s + 1, \dots, 3r - 2s - \sigma; \\ i_6 &= 3r - 2s - \sigma + 1, \dots, m; \end{aligned}$$

the set ξ_{i_1} not occurring if $\sigma = 0$, etc. Then (20) may be written

$$(20') \quad [14][23] \sim (-I)_{i_1}(I)_{i_2} \begin{pmatrix} O & -I \\ -I & O \end{pmatrix}_{i_3, i_4} (-I)_{i_5}(I)_{i_6}.$$

Let $[23] \sim K = (\kappa_{ab})$, $a, b = 1, \dots, 6$. Since K is commutative with (20'),

$$K = \begin{pmatrix} \kappa_{11} & O & \kappa_{13} & \kappa_{13} & \kappa_{15} & O \\ O & \kappa_{22} & \kappa_{23} & -\kappa_{23} & O & \kappa_{26} \\ \kappa_{31} & \kappa_{32} & \kappa_{33} & \kappa_{34} & \kappa_{35} & \kappa_{36} \\ \kappa_{31} & -\kappa_{32} & \kappa_{34} & \kappa_{33} & \kappa_{35} & -\kappa_{36} \\ \kappa_{51} & O & \kappa_{53} & \kappa_{53} & \kappa_{55} & O \\ O & \kappa_{62} & \kappa_{63} & -\kappa_{63} & O & \kappa_{66} \end{pmatrix}.$$

Now [14] may be obtained by transforming [23] by [13][24] and also by multiplying [23] by [14][23]. Equating the results for the corresponding transformations, we get

$$\kappa_{11} = \kappa_{15} = \kappa_{23} = \kappa_{32} = \kappa_{36} = \kappa_{51} = \kappa_{55} = \kappa_{63} = 0, \quad \kappa_{34} = -\kappa_{33}.$$

Hence, setting $\kappa = \kappa_{33}$, we have

$$(22) \quad K = UV, \quad U = \begin{pmatrix} O & \kappa_{13} & \kappa_{13} & O \\ \kappa_{31} & \kappa & -\kappa & \kappa_{35} \\ \kappa_{31} & -\kappa & \kappa & \kappa_{35} \\ O & \kappa_{53} & \kappa_{53} & O \end{pmatrix}_{i_1, i_3, i_4, i_5}, \quad V = \begin{pmatrix} \kappa_{22} & \kappa_{26} \\ \kappa_{62} & \kappa_{66} \end{pmatrix}_{i_2, i_6}.$$

We shall employ the symbols

$$(23) \quad \mu \equiv \begin{Bmatrix} \kappa_{13} \\ \kappa_{53} \end{Bmatrix}, \quad \nu \equiv \overbrace{\kappa_{31} \kappa_{35}}$$

to denote the square matrices of order $r - s$ defined as follows: The first σ rows of μ are composed of the elements of κ_{13} , the remaining $r - s - \sigma$ rows are composed of the elements of κ_{53} ; while ν is formed by annexing columns. By

combining the sets of variables ξ_{i_1} and ξ_{i_5} into one set $\xi_{i_1, 5}$, we have

$$(24) \quad U = \begin{pmatrix} \kappa & -\kappa & \nu \\ -\kappa & \kappa & \nu \\ \mu & \mu & O \end{pmatrix}_{i_3, i_4, i_1, 5}$$

Hence $U^2 = I$ if and only if

$$(25) \quad \mu\nu = \frac{1}{2}I, \quad \kappa^2 = \frac{1}{4}I.$$

Now $[12][23]$ is of period 3. Hence must

$$(26) \quad (C_{\sigma+1} \cdots C_s V)^3 = I$$

and $(CU)^3 = I$, where $C = C_1 \cdots C_\sigma C_{s+1} \cdots C_r$. For U given by (22), the conditions for $(CU)^2 = UC$ are seen to be

$$(27) \quad 2\kappa_{13}\kappa = -\kappa_{13}, \quad 2\kappa_{33}\kappa = \kappa_{33}, \quad 2\kappa\kappa_{31} = -\kappa_{31}, \quad 2\kappa\kappa_{35} = \kappa_{35}, \quad \kappa_{35}\kappa_{53} - \kappa_{31}\kappa_{13} = \kappa.$$

The first two of these conditions give

$$(28) \quad \mu\kappa = \delta\mu,$$

where δ is a square matrix all of whose non-diagonal elements are zero, while in the main diagonal the first σ elements are $-\frac{1}{2}$, and the remaining $r-s-\sigma$ elements are $+\frac{1}{2}$.

We next normalize the linear group by a transformation of variables. We multiply all matrices on the left by M and on the right by M^{-1} , where $M = (\mu)_{i_3}(\mu)_{i_4}$. Evidently (18)–(20) are unaltered. Then (24) becomes a matrix in which κ, μ, ν are replaced by $\mu\kappa\mu^{-1}, I, \mu\nu$, respectively. Hence by (25) and (28), the new U is

$$(29) \quad U = \begin{pmatrix} \delta & -\delta & \frac{1}{2}I \\ -\delta & \delta & \frac{1}{2}I \\ I & I & O \end{pmatrix}_{i_3, i_4, i_1, 5}$$

The remaining conditions (25) and (27) are seen to be satisfied. The characteristic equation of (29) is seen to have -1 as a root of multiplicity $r-s+\sigma$. Hence by (17) that of V has -1 as root of multiplicity $s-\sigma$.

THEOREM. *In every representation of the symmetric group S_4 , as a linear homogeneous group in a field not having modulus 2, we may, after a suitable transformation of variables, take the correspondence of generators to be (18)–(20) and $[23] \sim UV$, where U is given by (29) and V is a transformation $V_{i_2, 6}$ subject to condition (26) and having -1 as a root of multiplicity $s-\sigma$ of its characteristic equation.*

10. A transformation is commutative with (18), (19), and UV if and only

if it has the form

$$(30) \quad T_{i_3} T_{i_4} T_{i_{1,5}} Q_{i_2} R_{i_6}, \quad T = \begin{pmatrix} A & O \\ O & B \end{pmatrix},$$

where A and B are square matrices of orders σ and $r - s - \sigma$, respectively.

If $q \geq 6$, let $[56] \sim S$. By transforming the linear group by a transformation of type (30), we may express S as a product of C 's, without disturbing the earlier correspondences. Hence we may set

$$(31) \quad [56] \sim \prod_{i=1}^{\sigma_1} C_{s+i} C_{r+i} C_i \cdot \prod_{i=1}^{\sigma_2} C_{s+\sigma+i} C_{r+\sigma+i} C_{2r-s+i} \cdot \prod_{i=1}^{\sigma_3} C_{\sigma+i} \cdot \prod_{i=1}^{\sigma_4} C_{3r-2s+\sigma+i},$$

where

$$(32) \quad 0 \leq \sigma_1 \leq \sigma, \quad 0 \leq \sigma_2 \leq r - s - \sigma, \quad 0 \leq \sigma_3 \leq s - \sigma, \quad 0 \leq \sigma_4,$$

$$(33) \quad 3(\sigma_1 + \sigma_2) + \sigma_3 + \sigma_4 = r.$$

Now (18₁) and (31) have $2\sigma_1 + \sigma_2 + \sigma_3$ factors C in common, while the products (18) have s factors in common. Hence

$$(34) \quad 2\sigma_1 + \sigma_2 + \sigma_3 = s.$$

11. The main object of the paper is to determine the minimum number of variables upon which the symmetric group $S_{q!}$ can be represented. For this purpose it will be seen (§§ 19, 20) to be sufficient to know the representations in the case $r = 1$, whence $s = 0$. We shall assume merely that $s = 0$, as the specialization of r does not materially simplify the discussion.

For $s = 0$, we have $\sigma = 0$. Then $V = I$ since $V^2 = I$ and since all the roots of the characteristic equation are $+1$. Hence

$$(35) \quad [12] \sim C_1 \cdots C_r, \quad [34] \sim C_{r+1} \cdots C_{2r}, \quad [23] \sim U_{1, \dots, 3r},$$

the matrix of U being given by (29) for $\delta = \frac{1}{2}I$. Hence

$$(36) \quad U_{1, \dots, 3r}: \xi'_i = \xi_i + \omega_i, \quad \xi'_{r+i} = \xi_{r+i} + \omega_i, \quad \xi'_{2r+i} = \xi_{2r+i} - 2\omega_i \quad (i=1, \dots, r),$$

$$(37) \quad \omega_i = -\frac{1}{2}\xi_i - \frac{1}{2}\xi_{r+i} + \frac{1}{2}\xi_{2r+i}, \quad \omega'_i = -\omega_i \text{ under } U.$$

In § 10 we now have $\sigma_1 = \sigma_2 = \sigma_3 = 0$, $\sigma_4 = r$. Hence if $q \geq 6$,

$$(38) \quad [56] \sim C_{3r+1} \cdots C_{4r}.$$

Since $[36][45]$ is commutative with $[12]$ and $[34][56]$, and since its transform by $[56]$ and its product by $[34][56]$ both equal $[35][46]$, we have

$$[36][45] \sim T = A_{1, \dots, r} B_{r+1, \dots, 2r, 3r+1, \dots, 4r} C, \quad B = \begin{pmatrix} O & \beta \\ \beta^{-1} & O \end{pmatrix},$$

where β is a square matrix of order r , and

$$(39) \quad C = (\gamma_{ij}), \quad C^2 = I \quad (i, j = 2r+1, \dots, 3r, 4r+1, \dots, m).$$

Transforming the group by $(\beta)_{3r+1, \dots, 4r}$, we may set $\beta = I$. Then the characteristic determinant B_ρ of B equals $(\rho^2 - 1)^r$. If $A_\rho = 0$ has t roots -1 , then $C_\rho = 0$ has $r - t$ roots -1 , since $[36][45]$ is conjugate with $[12][34]$. Then $[12][36][45]$ has $r - t + r - t$ roots -1 , but is conjugate with $[12][34][56]$ with $3r$ roots -1 ; hence $t = 0$, $A = I$. Thus

$$(40) \quad [36][45] \sim T = \prod_{i=1}^r (\xi_{r+i} \xi_{3r+i}) \cdot C \quad (C_\rho \text{ with } r \text{ roots } -1).$$

Let $[45] \sim L$. We shall determine L by a device which brings to light its essential properties. The product

$$[36][45] \cdot [23] \cdot [34] \cdot [56]$$

transforms $[23]$ into $[45]$. Let $K = C_{r+1} \cdots C_{2r} C_{3r+1} \cdots C_{4r}$. Then the product $P = TUK$ transforms U into L . Hence $P^{-1} = KUT$ replaces the invariants of U by invariants of L , and replaces ω_i , given by (37), by a function which L must multiply by -1 , namely,

$$\tau_i = -\frac{1}{4}\xi_i - \frac{1}{4}\xi_{r+i} - \frac{1}{4}\xi_{2r+i} + \frac{1}{2}\xi_{3r+i} + \frac{1}{2} \sum_{j=1}^r \gamma_{2r+i, 2r+j} (\xi_j - \xi_{r+j}) + \frac{1}{2} \sum_{j=4r+1}^m \gamma_{2r+i, j} \xi_j.$$

Applying P^{-1} to the invariants $\xi_{r+i} + \frac{1}{2}\omega_i$ and ξ_{3r+i} of U , we get

$$-\xi_{3r+i} + \frac{1}{2}\tau_i, \quad \omega_i \quad (i=1, \dots, r).$$

Since C replaces $\sum \gamma_{ij} \xi_j$ by ξ_i by (39), P^{-1} replaces the invariants

$$\sum_{j=1}^r \gamma_{i, 2r+j} (\xi_{2r+j} - \omega_j) + \sum_{j=4r+1}^m \gamma_{ij} \xi_j \quad (i=2r+1, \dots, 3r, 4r+1, \dots, m)$$

of U by the following invariants of L :

$$(41) \quad \xi_i - \xi_{r+i} - \sum_{j=1}^r \gamma_{2r+i, 2r+j} \tau_j \quad (i=1, \dots, r), \quad \xi_i - \sum_{j=1}^r \gamma_{i, 2r+j} \tau_j \quad (i=4r+1, \dots, m).$$

Since $[45]$ is commutative with $[12]$, L must be commutative with $C_1 \cdots C_r$. Hence L replaces ξ_1, \dots, ξ_r by functions of the same, while the function by which L replaces ξ_i ($t > r$) is independent of ξ_1, \dots, ξ_r . Hence by the invariance of $\omega_1, \dots, \omega_r$, L leaves fixed ξ_1, \dots, ξ_r . But L must multiply each τ_i by -1 ; hence the τ_i are independent of ξ_1, \dots, ξ_r , so that

$$(42) \quad \gamma_{2r+i, 2r+i} = \frac{1}{2}, \quad \gamma_{2r+i, 2r+j} = 0 \quad (i, j=1, \dots, r; i \neq j).$$

Suitable linear combinations of the above invariants of L give

$$\xi_i, \quad \xi_{r+i} + \frac{1}{2}\tau_i, \quad \xi_{2r+i} - \xi_{r+i}, \quad \xi_{3r+i} - \frac{1}{2}\tau_i \quad (i=1, \dots, r).$$

In view of these and (41₂), the explicit form of L is

$$(43) \quad \delta\xi_{r+i} = \tau_i, \quad \delta\xi_{2r+i} = \tau_i, \quad \delta\xi_{3r+i} = -\tau_i \quad (i=1, \dots, r), \quad \delta\xi_i = -2 \sum_{j=1}^r \gamma_{i, 2r+j} \tau_j \\ (i=4r+1, \dots, m),$$

$$(44) \quad \tau_i = -\frac{1}{2}\xi_{r+i} - \frac{1}{4}\xi_{2r+i} + \frac{1}{2}\xi_{3r+i} + \frac{1}{2} \sum_{j=4r+1}^m \gamma_{2r+i, j} \xi_j,$$

where $\delta\xi \equiv \xi' - \xi$. Now L actually multiplies each τ_i by -1 if and only if *

$$(45) \quad \sum_{j=4r+1}^m \gamma_{2r+i, j} \gamma_{j, 2r+k} = \frac{3}{4} \delta_{ik} \quad (i, k=1, \dots, r),$$

where, in KRONECKER's notation, $\delta_{ii} = 1$, $\delta_{ik} = 0$ ($i \neq k$).

Since L was shown to leave each ω_i invariant, and since U evidently leaves each τ_i invariant, L and U are commutative. Since $LC_{r+1} \dots C_{2r}$ and $LC_{3r+1} \dots C_{4r}$ replace τ_i by ξ_{r+i} and $-\xi_{3r+i}$, respectively, they are easily seen to have period 3. Hence the correspondence given by (35), (38), and [45] $\sim L$, define a simple isomorphism between $S_{\delta!}$ and an m -ary linear group.

12. We may now readily treat the case when q is general:

$$(46) \quad q = 4\kappa + \kappa' \quad (0 \leq \kappa' < 4).$$

By the proof for [56], any transposition $[ij]$, $i > 4$, $j > 4$, corresponds to a transformation on the variables ξ_k ($k > 3r$). Hence we may set

$$(47) \quad [56] \sim \Pi C_{3r+i}, \quad [67] \sim U_{3r+1, \dots, 6r}, \quad [78] \sim \Pi C_{4r+i}; \\ [9, 10] \sim \Pi C_{6r+i}, \quad [10, 11] \sim U_{6r+1, \dots, 9r}, \quad [11, 12] \sim \Pi C_{7r+i}; \dots \\ [4\kappa - 3, 4\kappa - 2] \sim \Pi C_{(3\kappa-3)r+i}, \quad [4\kappa - 2, 4\kappa - 1] \sim U_{(3\kappa-3)r+1, \dots, 3\kappa r}, \\ [4\kappa - 1, 4\kappa] \sim \Pi C_{(3\kappa-2)r+i},$$

where for each product $i = 1, \dots, r$. Each of the κ "triples" (35) and (47) defines a simple isomorphism between the symmetric group on four letters and a linear group on $3r$ variables. It remains to insert the connecting "links" [45] $\sim L_1$, [89] $\sim L_2$, ..., and when $\kappa' > 0$ in (46) to extend the series beyond these κ triples (§§ 14-16).

In § 11 the only normalization was the transformation by $(\beta)_{3r+1, \dots, 4r}$. We here accomplish this normalization by transforming the linear group by

$$(\beta)_{3r+1, \dots, 4r} (\beta)_{4r+1, \dots, 5r} (\beta)_{5r+1, \dots, 6r},$$

and hence preserve the correspondences (35) and (47). Then L_1 is given by (43), subject to (44) and (45). Now L_1 must be commutative with all the transformations (47) except the first. Thus L_1 does not affect the variables

* These conditions also follow from (39) and (42).

ξ_i ($i = 6r + 1, \dots, 3\kappa r$), in view of the triples other than the first, nor ξ_i ($i = 4r + 1, \dots, 5r$), in view of [78]. Finally, L_1 must be commutative with $U = U_{3r+1, \dots, 6r}$. The necessary and sufficient conditions are that U leave unaltered each τ_i and that L_1 leave unaltered the functions

$$-\frac{1}{2}\xi_{3r+i} - \frac{1}{2}\xi_{4r+i} + \frac{1}{2}\xi_{5r+i} \quad (i = 1, \dots, r),$$

which U multiplies by -1 . Hence

$$(48) \quad \gamma_{2r+i, 5r+j} = \frac{1}{2}\delta_{ij}, \quad \gamma_{5r+i, 2r+j} = \frac{1}{2}\delta_{ij} \quad (i, j = 1, \dots, r).$$

Then relations (45) become

$$(49) \quad \sum_{j=3\kappa r+1}^m \gamma_{2r+i, j} \gamma_{j, 2r+k} = \frac{1}{2}\delta_{ik} \quad (i, k = 1, \dots, r).$$

In the final terms of (43) and (44) we may restrict i and j to the values $3\kappa r + 1, \dots, m$, provided we insert the term $\frac{1}{4}\xi_{5r+i}$ in (44), and $8\xi_{5r+l} = -\tau_i$ in (43).

We next exhibit L_1 in a notation better suited for the further discussion. We set

$$m = 3\kappa r + \mu, \quad \tau_i = \tau_{i1}, \quad \gamma_{3\kappa r+i, 2r+j} = \frac{1}{2}\beta_{ij1}, \quad \gamma_{2r+j, 3\kappa r+i} = \frac{1}{2}\alpha_{j1i},$$

for $i = 1, \dots, \mu$; $j = 1, \dots, r$. Then

$$\begin{aligned} L_1: \quad \delta\xi_{r+i} &= \delta\xi_{2r+i} = \tau_{i1}, \quad \delta\xi_{3r+i} = \delta\xi_{5r+i} = -\tau_{i1} \quad (i = 1, \dots, r), \\ \delta\xi_{3\kappa r+i} &= -\sum_{j=1}^r \beta_{ij1} \tau_{j1} \quad (i = 1, \dots, \mu), \\ \tau_{i1} &= -\frac{1}{2}\xi_{r+i} - \frac{1}{4}\xi_{2r+i} + \frac{1}{2}\xi_{3r+i} + \frac{1}{4}\xi_{5r+i} + \frac{1}{4}\sum_{j=1}^{\mu} \alpha_{ij} \xi_{3\kappa r+j} \quad (i = 1, \dots, r), \\ \sum_{j=1}^{\mu} \alpha_{ij} \beta_{jkl} &= 2\delta_{ik} \quad (i, k = 1, \dots, r). \end{aligned}$$

The link $[4t, 4t + 1] \sim L_t$ may be obtained from L_1 by adding $3(t-1)r$ to the subscripts $\leq 3\kappa r$ of the ξ 's. Hence, for $t = 1, \dots, \kappa - 1$,

$$(50) \quad L_t: \delta\xi_{(3t-2)r+i} = \delta\xi_{(3t-1)r+i} = \tau_{it}, \quad \delta\xi_{3tr+i} = \delta\xi_{(3t+2)r+i} = -\tau_{it} \quad (i = 1, \dots, r),$$

$$\delta\xi_{3\kappa r+j} = -\sum_{k=1}^r \beta_{jkt} \tau_{kt} \quad (j = 1, \dots, \mu),$$

$$(51) \quad \tau_{it} = -\frac{1}{2}\xi_{(3t-2)r+i} - \frac{1}{4}\xi_{(3t-1)r+i} + \frac{1}{2}\xi_{3tr+i} + \frac{1}{4}\xi_{(3t+2)r+i} + \frac{1}{4}\sum_{j=1}^{\mu} \alpha_{ij} \xi_{3\kappa r+j},$$

$$(52) \quad \sum_{j=1}^{\mu} \alpha_{ij} \beta_{jkt} = 2\delta_{ik} \quad (i, k = 1, \dots, r).$$

Now L_t and L_s are commutative if and only if each leaves fixed the τ_i functions belonging to the other. According as $s = t + 1$ or $s > t + 1$, the condi-

tions are, respectively,

$$(53) \quad \sum_{j=1}^{\mu} \alpha_{it+ij} \beta_{jkt} = \delta_{ik}, \quad \sum_{j=1}^{\mu} \alpha_{itj} \beta_{jkt+1} = \delta_{ik},$$

$$(54) \quad \sum_{j=1}^{\mu} \alpha_{isj} \beta_{jkt} = 0, \quad \sum_{j=1}^{\mu} \alpha_{itj} \beta_{jks} = 0 \quad (s \geq t+2),$$

holding for $s, t = 1, \dots, \kappa - 1; i, k = 1, \dots, r$.

13. The product of the two matrices

$$(55) \quad A_i = (\alpha_{itj}), \quad B_k = (\beta_{jkt}) \quad (t = 1, \dots, \kappa - 1; j = 1, \dots, \mu),$$

the first having $\kappa - 1$ rows and μ columns and the second having μ rows and $\kappa - 1$ columns, is a square matrix of order $\kappa - 1$:

$$(56) \quad P_{ik} = (\pi_{itl}^{ik}), \quad \pi_{itl}^{ik} \equiv \sum_{j=1}^{\mu} \alpha_{itj} \beta_{jkl} \quad (t, l = 1, \dots, \kappa - 1).$$

In view of (52)–(54), we have

$$\pi_{it}^{ik} = 2\delta_{ik}, \quad \pi_{t+1t}^{ik} = \pi_{t+1t+1}^{ik} = \delta_{ik}, \quad \pi_{st}^{ik} = \pi_{ts}^{ik} = 0 \quad (s \geq t+2).$$

Hence if $i \neq k$, P_{ik} is a matrix O all of whose elements are zero. Also each P_{ii} is the matrix

$$(57) \quad P = \begin{pmatrix} 2 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 2 \end{pmatrix},$$

the elements in the main diagonal being 2, those in the adjacent parallels being 1, and all the remaining elements being 0. If we set $|P| = \Delta_{\kappa-1}$ and expand according to the first row, we have

$$\Delta_{\kappa-1} = 2\Delta_{\kappa-2} - \Delta_{\kappa-3},$$

whence, by induction, $\Delta_{\kappa-1} = \kappa$. As in (23), we set

$$(58) \quad A = \left. \begin{matrix} A_1 \\ \vdots \\ A_r \end{matrix} \right\}, \quad B = \overbrace{B_1 \dots B_r}.$$

Since $A_i B_k = P_{ik}$, we have

$$(59) \quad AB = \begin{pmatrix} P & O & \dots & O \\ . & . & . & . & . & . \\ O & O & \dots & P \end{pmatrix}, \quad |AB| = \kappa^r.$$

First, let $\mu < (\kappa - 1)r$. We convert matrices A and B into square matrices.

of order $(\kappa - 1)r$ by adding columns of zero elements to the former and rows of zero elements to the latter. In view of their determinants, we have $0.0 = \kappa^r$. Hence the field F must have a modulus which divides κ .

Next, let $\mu < (\kappa - 2)r$. Drop the last row of each A_i and the last column of each B_i . Let A and B then become A^* and B^* . Hence

$$(59^*) \quad A^* B^* = \begin{pmatrix} P^* & O & \cdots & O \\ \cdot & \cdot & \cdot & \cdot \\ O & O & \cdots & P^* \end{pmatrix}, \quad |A^* B^*| = (\kappa - 1)^r,$$

where P^* is obtained from P by deleting the last row and last column. Thus $|P^*| = \Delta_{\kappa-2} = \kappa - 1$. We convert A^* and B^* into square matrices of order $(\kappa - 2)r$ by adding columns of zero elements to the former and rows of zero elements to the latter. Hence $0.0 = (\kappa - 1)^r$, in contradiction to the preceding case.

THEOREM. *For $q \geq 4\kappa$ we have $\mu \geq (\kappa - 1)r$ or $\mu \geq (\kappa - 2)r$, according as the field does not have or has a modulus which divides κ .*

By §§ 2-4 the symmetric group on 4κ letters can always be represented as a linear group G on $4\kappa - 1$ variables; and, if the modulus divides κ , as a linear group G' on $4\kappa - 2$ variables. By notation, $m \equiv 3\kappa r + \mu$. If F does not have a modulus dividing κ , the direct product of r groups G gives a representation for which the number of variables is $(4\kappa - 1)r = m$, with $\mu = (\kappa - 1)r$. If F has a modulus dividing κ , the direct product of l groups G and $r - l$ groups G' gives a representation for which the number of variables is

$$(4\kappa - 1)l + (4\kappa - 2)(r - l) = m, \quad \text{with} \quad \mu = (\kappa - 2)r + l.$$

Thus μ may have any of the values $(\kappa - 2)r, (\kappa - 2)r + 1, \dots$. In particular the limits which the theorem assigns to μ cannot be lowered.

The problem of the normalization of the groups is considered in §§ 22-24.

14. Let next $q \geq 4\kappa + 1$, and set $[4\kappa - 1, 4\kappa + 1] \sim S$. Then S must be commutative with the first $\kappa - 1$ triples (35) and (47), and with $\Pi C_{(3\kappa-3)r+i}$. The variables in the latter are not affected by S in view of the hypothesis of § 11. Hence

$$(60) \quad S: \quad \xi'_{(3\kappa-2)r+i} = \sum_{j=1}^v \sigma_{ij} \xi_{(3\kappa-2)r+j} \quad (i=1, \dots, v),$$

where $v = m - (3\kappa - 2)r$. Now

$$[4\kappa - 1, 4\kappa] \sim P = \prod_{i=1}^r C_{(3\kappa-2)r+i}.$$

Hence

$$(61) \quad [4\kappa, 4\kappa + 1] \sim T = SP S: \delta \xi_{(3\kappa-2)r+i} = -2 \sum_{j=1}^r \sigma_{ij} \tau_j \quad (i=1, \dots, v),$$

in which τ_i denotes the sum (60) for $i \leq r$. Next, T must be commutative with

$$U_{(3\kappa-3)r+1, \dots, 3\kappa r} : \quad \delta \xi_{(3\kappa-3)r+i} = \delta \xi_{(3\kappa-2)r+i} = \lambda_i, \quad \delta \xi_{(3\kappa-1)r+i} = -2\lambda_i, \\ \lambda_i = -\frac{1}{2}\xi_{(3\kappa-3)r+i} - \frac{1}{2}\xi_{(3\kappa-2)r+i} + \frac{1}{2}\xi_{(3\kappa-1)r+i} \quad (i=1, \dots, r),$$

in accord with (36), (37). But UT and TU replace $\xi_{(3\kappa-3)r+i}$ by equal functions if and only if T leaves λ_i unaltered, the conditions for which are

$$(62) \quad \sigma_{ij} = \sigma_{r+j} \quad (i, j=1, \dots, r).$$

Again, UT and TU replace $\xi_{(3\kappa-2)r+i}$ by equal functions if and only if U leaves unaltered the sum in (61). For $i=1, \dots, \nu, r$ of these sums are linearly independent since the σ_{ij} form the first r columns of the matrix of S . Hence U must leave unaltered each τ_j , so that

$$(63) \quad \sigma_{ji} = 2\sigma_{r+i} \quad (i, j=1, \dots, r).$$

Next, P must transform T into S . The conditions are

$$(64) \quad \delta_{ik} \pm 2 \sum_{j=1}^r \sigma_{ij} \sigma_{jk} = \sigma_{ik} \quad (i, k=1, \dots, \nu).$$

the sign being minus if and only if i and k are both $\leq r$ or both $> r$. Let first $k \leq r, i = r + \epsilon, \epsilon \leq r$; then, by (62), (64) becomes

$$2 \sum_{j=1}^r \sigma_{\epsilon j} \sigma_{jk} = \sigma_{\epsilon k},$$

Adding this to (64) for $i = \epsilon$, we get $\frac{1}{2}\delta_{\epsilon k} = \sigma_{\epsilon k}$. Hence by (62), (63),

$$(65) \quad \sigma_{ij} = \sigma_{r+j} = \frac{1}{2}\delta_{ij}, \quad \sigma_{ir+j} = \frac{1}{4}\delta_{ij} \quad (i, j=1, \dots, r).$$

Then conditions (64) become identities unless $i > r, k > r$, while then the σ_{ij} involved do not occur in (61). Hence we need not consider further the conditions (64).

To make our notations uniform with those at the end of § 12, we set

$$T = T_{\kappa}, \quad \tau_i = -\tau_{i\kappa}, \quad \sigma_{2r+j, k} = -\frac{1}{2}\beta_{jk\kappa}, \quad \sigma_{i, 2r+j} = -\frac{1}{4}\alpha_{i\kappa j}.$$

Then the preceding results give

$$(66) \quad T_{\kappa} : \delta \xi_{(3\kappa-2)r+i} = \delta \xi_{(3\kappa-1)r+i} = \tau_{i\kappa}, \quad \delta \xi_{3\kappa r+j} = -\sum_{k=1}^r \beta_{jk\kappa} \tau_{k\kappa} \quad \left(\begin{matrix} i=1, \dots, r \\ j=1, \dots, \mu \end{matrix} \right),$$

$$(67) \quad \tau_{i\kappa} = -\frac{1}{2}\xi_{(3\kappa-2)r+i} - \frac{1}{4}\xi_{(3\kappa-1)r+i} + \frac{1}{4} \sum_{j=1}^{\mu} \alpha_{i\kappa j} \xi_{3\kappa r+j}.$$

Since T_{κ} must multiply $\tau_{i\kappa}$ by -1 , we have

$$(68) \quad \sum_{j=1}^{\mu} \alpha_{ikj} \beta_{jk\kappa} = 5\delta_k \quad (i, k=1, \dots, r).$$

The conditions that T_κ be commutative with $L_{\kappa-1}$ and L_t ($t < \kappa - 1$) are

$$(69) \quad \sum_{j=1}^{\mu} \alpha_{i\kappa j} \beta_{jk\kappa-1} = \delta_{ik}, \quad \sum_{j=1}^{\mu} \alpha_{i\kappa-1j} \beta_{jk\kappa} = \delta_{ik}, \quad \left(\begin{matrix} i, k=1, \dots, r \\ t=1, \dots, \kappa-2 \end{matrix} \right)$$

$$(70) \quad \sum_{j=1}^{\mu} \alpha_{i\kappa j} \beta_{jkt} = 0, \quad \sum_{j=1}^{\mu} \alpha_{itj} \beta_{jk\kappa} = 0.$$

We proceed as in § 13, with an additional value κ for t . Thus in (55), A_i now has an additional row, B_k an additional column, while in (56) and (57) there is an additional row and column, the new diagonal element being 5, the element preceding 5 being 1, that above 5 being 1, and the remaining elements being zero, by (68)–(70). Expanding $|\pi_{tt'}|$ according to the last row, we get

$$5\Delta_{\kappa-1} - \Delta_{\kappa-2} = 5\kappa - (\kappa - 1) = 4\kappa + 1.$$

THEOREM. For $q \geq 4\kappa + 1$ we have $\mu \geq \kappa r$ or $\mu \geq (\kappa - 1)r$, according as the field does not have or has a modulus which divides $4\kappa + 1$.

15. Let next $q \geq 4\kappa + 2$. To $[4\kappa + 1, 4\kappa + 2]$ corresponds a transformation commutative with the κ triples (35) and (47) and hence not affecting ξ_i ($i = 1, \dots, 3\kappa r$). Applying a transformation on the remaining variables, we may set

$$(71) \quad [4\kappa + 1, 4\kappa + 2] \sim Q = \prod_{i=1}^r C_{3\kappa r+i}.$$

Since the latter must be commutative with L_t , we have

$$(72) \quad \alpha_{ijt} = 0, \quad \beta_{ijt} = 0 \quad (i, j = 1, \dots, r; t = 1, \dots, \kappa - 1).$$

Since $[4\kappa, 4\kappa + 1] \sim T_\kappa$, given by (66), $T_\kappa Q$ must be of period 3. The necessary and sufficient conditions are

$$(73) \quad \sum_{j=1}^r \alpha_{i\kappa j} \beta_{jk\kappa} = 2\delta_{ik} = \sum_{j=1}^r \alpha_{j\kappa k} \beta_{ij\kappa} \quad (i, k = 1, \dots, r).$$

Thus $|\alpha| \neq 0$. We make the transformation of variables

$$\xi_{3\kappa r+i}^* = \frac{1}{2} \sum_{j=1}^r \alpha_{i\kappa j} \xi_{3\kappa r+j} \quad (i = 1, \dots, r).$$

Of the preceding transformations, the only one altered is T_κ . For the latter, $\delta \xi_{3\kappa r+i}^* = -\tau_{i\kappa}$. The effect of this normalization is the replacement of conditions (73) by

$$(74) \quad \beta_{jk\kappa} = \delta_{jk}, \quad \alpha_{j\kappa k} = 2\delta_{jk} \quad (j, k = 1, \dots, r).$$

The remaining parameters of our transformations define the matrices

$$(75) \quad A_i = (\alpha_{itj}), \quad B_i = (\beta_{ji\mu}) \quad (t = 1, \dots, \kappa; j = r+1, \dots, \mu; i = 1, \dots, r).$$

These parameters are subject to conditions (52)–(54), (69), (70), in which, by

(72), we may now take $j = r + 1, \dots, \mu$, and to the conditions

$$(76) \quad \sum_{j=r+1}^{\mu} \alpha_{ijk} \beta_{jk\kappa} = 3\delta_{ik} \quad (i, k = 1, \dots, r),$$

which follow from (68) and (74). The statements at the end of § 14 hold here if we replace 5 by 3; in particular, $|\pi| = 2\kappa + 1$. In applying the argument of § 13, the two cases to consider are now $\mu - r < \kappa r$ and $\mu - r < (\kappa - 1)r$.

THEOREM. *For $q \geq 4\kappa + 2$, we have $\mu \geq (\kappa + 1)r$ or $\mu \geq \kappa r$, according as the field does not have or has a modulus which divides $2\kappa + 1$.*

Note that (66) and (67) simplify, in view of (74):

$$(66') \quad T_{\kappa}: \delta\xi_{(3\kappa-2)r+i} = \delta\xi_{(3\kappa-1)r+i} = \tau_{i\kappa}, \quad \delta\xi_{3\kappa r+i} = -\tau_{i\kappa} \quad (i = 1, \dots, r),$$

$$\delta\xi_{3\kappa r+j} = -\sum_{k=1}^r \beta_{jk\kappa} \tau_{k\kappa} \quad (j = r+1, \dots, \mu),$$

$$(67') \quad \tau_{i\kappa} = -\frac{1}{2}\xi_{(3\kappa-2)r+i} - \frac{1}{4}\xi_{(3\kappa-1)r+i} + \frac{1}{2}\xi_{3\kappa r+i} + \frac{1}{4}\sum_{j=r+1}^{\mu} \alpha_{ijk} \xi_{3\kappa r+j}.$$

16. Finally, let $q = 4\kappa + 3$. Since a transformation commutative with the κ triples affects only ξ_i ($i > 3\kappa r$), we have

$$(77) \quad [4\kappa + 1, 4\kappa + 3] \sim E: \xi'_{3\kappa r+i} = \sum_{j=1}^{\mu} \epsilon_{ij} \xi_{3\kappa r+j} \quad (i = 1, \dots, \mu).$$

Then, by (71),

$$(78) \quad [4\kappa + 2, 4\kappa + 3] \sim R = EQE: \delta\xi_{3\kappa r+i} = -2 \sum_{j=1}^r \epsilon_{ij} \omega_j \quad (i = 1, \dots, \mu),$$

in which ω_i denotes the sum (77) for $i \leq r$. Now Q must transform R into E . As in (64), the conditions are

$$(79) \quad \delta_{ik} \pm 2 \sum_{j=1}^r \epsilon_{ij} \epsilon_{jk} = \epsilon_{ik} \quad (i, k = 1, \dots, \mu),$$

the sign being minus if and only if i and k are both $\leq r$ or both $> r$. Set

$$(80) \quad e = (\epsilon_{ij}), \quad e_{\rho} = e - \rho I \quad (i, j = 1, \dots, r).$$

In view of relations (79) for $i, k = 1, \dots, r$, we have

$$(81) \quad e_{\rho} e_{\sigma} = \left(\frac{1}{2} + \rho\sigma\right) I + fe \quad (f = -\frac{1}{2} - \rho - \sigma).$$

Set $\Delta_{\rho} = |e_{\rho}|$. Taking $f = 0$, we have

$$(82) \quad \Delta_{\rho} \Delta_{-\frac{1}{2}-\rho} = \left[\frac{1}{2} + \rho\left(-\frac{1}{2} - \rho\right)\right]^r = (1 + \rho)^r \left(\frac{1}{2} - \rho\right)^r.$$

We next prove* that $\Delta_{\rho} = 0$ actually has the root $\rho = \frac{1}{2}$. For a fixed value of k ($k > r$), equations (79), with $i = 1, \dots, r$, may be written

$$(83) \quad \epsilon_{i1} \epsilon_{1k} + \dots + \left(\epsilon_{ii} - \frac{1}{2}\right) \epsilon_{ik} + \dots + \epsilon_{ir} \epsilon_{rk} = 0.$$

* This is obvious if the modulus is 3, since $-1 \equiv \frac{1}{2}$.

For a fixed value of i ($i > r$), equations (79), with $k = 1, \dots, r$, are

$$(84) \quad \epsilon_{ik} \epsilon_{i1} + \dots + (\epsilon_{kk} - \tfrac{1}{2}) \epsilon_{ik} + \dots + \epsilon_{rk} \epsilon_{ir} = 0.$$

Hence, if $\Delta_{\frac{1}{2}} \neq 0$, then $\epsilon_{ik} = 0$ ($i \leq r, k > r$), $\epsilon_{ik} = 0$ ($i > r, k \leq r$), so that E would be commutative with Q , and the isomorphism would fail.

It follows that $\Delta_p = 0$ has an l -fold root $\frac{1}{2}$ and an $(r-l)$ -fold root -1 , where $l \geq 1$, while $l = r$ if the field has modulus 3. Applying* a transformation on the variables $\xi_{3\kappa r+i}$ ($i = 1, \dots, r$), we may, in view of the theory of canonical forms, normalize e and set

$$(85) \quad \epsilon_{ij} = 0 \ (j \neq i, i-1), \quad \epsilon_{ii} = \tfrac{1}{2} \ (i = 1, \dots, l), \quad \epsilon_{ii} = -1 \ (i = l+1, \dots, r), \\ \epsilon_{i+l} = 0.$$

Then equations (79), for $i, k = 1, \dots, r$, reduce to

$$(86) \quad 3\epsilon_{ii-1} = 0 \ (i \neq l+1), \quad \epsilon_{ii-1} \epsilon_{i-1i-2} = 0 \ (i = 1, \dots, r).$$

Let $\kappa > 0$. Then R must be commutative with T_κ , given by (66'). By an argument similar to that with U in § 14, the conditions are that

$$(87) \quad R \text{ leaves fixed each } \tau_{i\kappa}, T_\kappa \text{ each } \omega_i \quad (i = 1, \dots, r).$$

Suppose first that the field does not have modulus 3. Then by (85), (86), $\epsilon_{ii-1} = 0$ ($i = 2, \dots, r$). Hence (83) and (84) reduce to

$$(88) \quad \epsilon_{ik} = 0 \ (i = l+1, \dots, r; k > r), \quad \epsilon_{ik} = 0 \ (i > r; k = l+1, \dots, r).$$

Hence E and R are products of $\Pi C_{3\kappa r+i}$ by transformations not affecting

$$(89) \quad \xi_{3\kappa r+i} \quad (i = l+1, \dots, r).$$

Then, by † (87), T_κ leaves unaltered the variables (89). But, for Q defined by (71), $T_\kappa Q$ must be of period 3. Hence $l = r$, and

$$(90) \quad (\epsilon_{ij}) = \tfrac{1}{2} I \quad (i, j = 1, \dots, r).$$

Next let the field have modulus 3. Then $\epsilon_{ii} = -1$ ($i \leq r$). Suppose that $\epsilon_{ii-1} \neq 0$ for a fixed value of i , $2 \leq i \leq r$. Then by (86) and (83),

$$\epsilon_{i-1i-2} = 0, \quad \epsilon_{i-1k} = 0 \quad (k = r+1, \dots, \mu).$$

Then $\omega_{i-1} = -\xi_{3\kappa r+i-1}$; so that, by (87), T_κ leaves $\xi_{3\kappa r+i-1}$ unaltered. Then $T_\kappa Q$ is not of period 3, contrary to the isomorphism. Hence each $\epsilon_{ii-1} = 0$ ($i \leq r$), and relation (90) holds.

Having established (90), we introduce notations uniform with those of the preceding sections. We set

$$R = T_{\kappa+1}, \quad \omega_i = -\tau_{i\kappa+1}, \quad \epsilon_{ji} = -\tfrac{1}{2}\beta_{jik+1}, \quad \epsilon_{ij} = -\tfrac{1}{4}\alpha_{i\kappa+1j} \quad (i \leq r; j > r).$$

* If $\kappa > 0$, we forego for the present the normalization (74) of T_κ .

† To give a direct proof, we note that T_κ multiplies each variable (89) by ± 1 , and that $\pm 1 = +1$ by the hypothesis in § 11.

Then by (78), (90), and the definition of ω_i as the sum (77),

$$(91) \quad T_{\kappa+1} : \delta \xi_{3\kappa r+i} = \tau_{i\kappa+1}, \quad \delta \xi_{3\kappa r+j} = - \sum_{k=1}^r \beta_{jk\kappa+1} \tau_{k\kappa+1} \quad (i=1, \dots, r; j=r+1, \dots, \mu),$$

$$(92) \quad \tau_{i\kappa+1} = -\frac{1}{2} \xi_{3\kappa r+i} + \frac{1}{4} \sum_{j=r+1}^{\mu} \alpha_{i\kappa+1j} \xi_{3\kappa r+j}.$$

In view of its origin, $T_{\kappa+1}$ must multiply $\tau_{i\kappa+1}$ by -1 , whence

$$(93) \quad \sum_{j=r+1}^{\mu} \alpha_{i\kappa+1j} \beta_{jk\kappa+1} = 6\delta_{ik} \quad (i, k=1, \dots, r).$$

Without altering (90) we may make the normalization in § 15, by means of which T_{κ} takes the form (66'). In view of (87), T_{κ} and $T_{\kappa+1}$ are commutative if and only if

$$(94) \quad \sum_{j=r+1}^{\mu} \alpha_{i\kappa+1j} \beta_{jk\kappa} = 2\delta_{ik}, \quad \sum_{j=r+1}^{\mu} \alpha_{i\kappa j} \beta_{jk\kappa+1} = 2\delta_{ik} \quad (i, k=1, \dots, r).$$

Finally, $T_{\kappa+1}$ is commutative with L_t , given by (50), (51), (72), if and only if

$$(95) \quad \sum_{j=r+1}^{\mu} \alpha_{i\kappa+1j} \beta_{jk t} = 0, \quad \sum_{j=r+1}^{\mu} \alpha_{i t j} \beta_{jk\kappa+1} = 0 \quad (i, k=1, \dots, r; t=1, \dots, \kappa-1).$$

We proceed as at the end of § 15. We consider matrices (75) for $t=1, \dots, \kappa+1$, viz., with an additional row in A_i and an additional column in B_i , the new elements satisfying (93)–(95). Thus, for $i \neq k$, $A_i B_k$ is a matrix all of whose elements are zero; while

$$(96) \quad A_i B_i = \begin{pmatrix} 2 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 3 & 2 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 2 & 6 \end{pmatrix},$$

a square matrix of order $\kappa+1$, whose determinant equals (§§ 13, 15)

$$6(2\kappa+1) - 2^2 \Delta_{\kappa-1} = 2(4\kappa+3).$$

Considering as in § 13 the cases $\mu-r < (\kappa+1)r$ and $\mu-r < \kappa r$, we obtain the following

THEOREM. *For $q=4\kappa+3$, we have $\mu \geq (\kappa+2)r$ or $\mu \geq (\kappa+1)r$, according as the field does not have or has a modulus which divides q .*

17. Under the hypothesis made in § 11 that $s=0$, we have exhibited in §§ 11–16 the correspondence of generators in any simple isomorphism between

the symmetric group on q letters and an m -ary linear homogeneous group in a field not having modulus 2, and have obtained lower limits on $\mu \equiv m - 3\kappa r$. The latter results may be combined into the following

THEOREM. *The minimum value of m is $(q-1)r$ or $(q-2)r$, according as the field does not have or has a modulus which divides q .*

For $r = 1$, the hypothesis $s = 0$ is satisfied and we have the

COROLLARY. *In any representation of the symmetric group on q letters as an m -ary linear homogeneous group, such that a transposition corresponds to a transformation conjugate with C_1 , it is necessary that $m \geq q - 2$, while $m = q - 2$ only when the field has a modulus which divides q .*

18. Principle of duality. If the general m -ary linear homogeneous group $GLH(m, F)$ in a field F , not having modulus 2, contains a subgroup $G_q^{(r)}$ of symmetric type, such that a transposition corresponds to a transformation conjugate with $C_1 \cdots C_r$, then $GLH(m, F)$ contains a subgroup $G_q^{(m-r)}$.

As this is obviously true when $q = 2$, we set $q > 2$. Then there is no invariant substitution, so that $C = C_1 \cdots C_m$ cannot occur in $G_q^{(r)}$. In particular, $r < m$.

Let the even substitutions correspond to the transformations e_1, e_2, \dots of $G_q^{(r)}$, and the odd substitutions to o_1, o_2, \dots . Then

$$e_1, e_2, \dots, o_1 C, o_2 C, \dots$$

are all distinct and form an isomorphic group $G_q^{(m-r)}$.

19. **LEMMA.** *The symmetric group on $m+3$ letters cannot be represented as an m -ary linear homogeneous group in a field not having modulus 2.*

The proof proceeds by induction from $m-2$ to m , the lemma being evidently true for $m=1$, and true for $m=2$ by § 17, since then $r=1$ by § 18.

Suppose that there is a representation $G_{(m+3)}^{(r)}$. By §§ 17, 18 we may set

$$(97) \quad 2 \leq r \leq \frac{1}{2}m, \quad [12] \sim C_1 \cdots C_r.$$

Any transformation commutative with $C_1 \cdots C_r$ is necessarily a product $S_{1, \dots, r} S'_{r+1, \dots, m}$. Hence by § 7 the symmetric group on the $m+1$ letters $3, \dots, m+3$ is simply isomorphic with a linear homogeneous group on r or $m-r$ variables. By (97), $r \leq m-2$, $m-r \leq m-2$. Hence the hypothesis for the induction is contradicted.

20. Suppose, finally, that the symmetric group on $m+2$ letters is representable as an m -ary linear homogeneous group in a field F not having modulus 2. If $r=1$ or $m-1$, F must have a modulus which divides $m+2$ (§ 17). If $1 < r < m-1$, we may assume that (97) holds. As in § 19, the symmetric group G on the m letters $3, \dots, m+2$ is simply isomorphic with a group on r

or else $m - r$ variables; while by the lemma there proved the number of variables is $\equiv m - 2$. For either alternative, it follows from (97₁) that $r = 2$. Then $m \equiv 4$, so that (§ 4 or §§ 17-19) G cannot be represented on $r = 2$ variables.

Hence by the proof given in § 7, there remain only two possibilities:

(i) The group G affects only the variables ξ_3, \dots, ξ_m ;

(ii) The transformations of G corresponding to even substitutions affect only the variables ξ_3, \dots, ξ_m ; while those corresponding to odd substitutions are products of transformations on ξ_3, \dots, ξ_m by a fixed transformation T , of period 2, on ξ_1 and ξ_2 .

For case (i), we have (18) with $r = 2, s = 0$. Hence by § 17, the minimum number of variables in a representation of $S_{(m+2)!}$ is $2m$. We may proceed directly and conclude from $[12] \sim C_1 C_2, [34] \sim C_3 C_4, [56] \sim C_5 C_6, \dots$ that at least $m + 2$ or $m + 1$ variables are necessary, according as $m + 2$ is even or odd.

For case (ii), we apply a transformation on ξ_1, ξ_2 , and set $T = C_1$, since obviously $T \neq C_1 C_2$. Applying a transformation on ξ_3, \dots, ξ_m , we may set $[34] \sim C_1 C_3, [56] \sim C_1 C_4$, and, as before, $[12] \sim C_1 C_2$. The case thus falls under § 9 with $r = 2, s = 1$. Then by (20) we may set $[14][23] \sim (\xi_2 \xi_3) C_2 C_3 C_k$, where $k = 1$ if $\sigma = 1, k = 4$ if $\sigma = 0$. Let $[23] \sim W$. Since $[23]$ is commutative with $[56]$ and $[14][23]$, we have $W = (a)_1(b)_4 S$, S affecting only $\xi_2, \xi_3, \xi_5, \dots$. Since $[12][23]$ is of period 3, we have $a = -1$. If $b = -1, [23]$ and $[56]$ both correspond to $C_1 C_4$. Hence $W = C_1 S$. It follows that $S_{(m+2)!}$ is represented as a subgroup of the direct product of $\{I, C_1\}$ and a group on ξ_2, \dots, ξ_m , and hence (§ 7) is simply isomorphic with a group on $m - 1$ variables. But this contradicts § 19.

Hence cases (i) and (ii) are both excluded.

THEOREM. *If the symmetric group on q letters is representable as a linear homogeneous group on $q - 2$ variables in a field F not having modulus 2, then $r = 1$ or $q - 3$, and F has a modulus which divides q .*

21. In view of §§ 8, 19, 20, we may state the complete

THEOREM. *Let F be an arbitrary field. Then the minimum number of variables for the representation of the symmetric group on q letters is $q - 1$ or $q - 2$, according as F has not or has a modulus which divides q . In the latter case exceptions arise for $q \leq 4$; when the modulus divides q , the minimum number of variables is 2 for $q = 2$ or 3, and 3 for $q = 4$.*

22. In order to obtain a clear insight into the nature of the linear groups exhibited in §§ 11-16, we shall make a normalization by a transformation of variables which does not disturb the correspondences (35) and (47). To normalize the L_i , given by (50), set

$$(98) \quad \eta_{3kr+i} = \sum_{j=1}^{\mu} \lambda_{ij} \xi_{3kr+j} \quad (i = 1, \dots, \mu).$$

Then, under L_t ,

$$(99) \quad \delta\eta_{3\kappa r+i} = - \sum_{k=1}^r \beta'_{ikt} \tau_{kt}, \quad \beta'_{ikt} = \sum_{j=1}^{\mu} \lambda_{ij} \beta_{jkt}.$$

Suppose first that the field does not have a modulus which divides κ . Then, by § 13, $\mu \equiv (\kappa - 1)r$. As in (55) and (58), set

$$(100) \quad B'_k = (\beta'_{jkt}), \quad B' = \overbrace{B'_1 \cdots B'_r}^{\quad} \quad (t=1, \dots, \kappa-1; j=1, \dots, \mu).$$

Thus $(\lambda)B = B'$. Now $|AB|$ equals the sum of all products of the determinants of order $(\kappa - 1)r$ formed from $(\kappa - 1)r$ columns of A by the corresponding determinants formed from $(\kappa - 1)r$ rows of B . But $|AB| \neq 0$ by (59). Hence, after making a suitable permutation of the variables $\xi_{3\kappa r+j}$, we may set $|\bar{B}| \neq 0$, where

$$(101) \quad \bar{B} = \overbrace{\bar{B}_1 \cdots \bar{B}_r}^{\quad}, \quad \bar{B}_k = (\beta_{jkt}) \quad [t=1, \dots, \kappa-1; j=1, \dots, (\kappa-1)r],$$

so that \bar{B}_k is composed of the first $(\kappa - 1)r$ rows of B_k . For the purpose of assigning an order to the β 's in the j th row of \bar{B} , we set

$$(102) \quad \beta_{jkt} \equiv \beta_{j, (\kappa-1)(k-1)+t}.$$

For a fixed value $\leq \mu$ of i , the equations

$$(103) \quad \beta'_{ikt} = \delta_{i, (\kappa-1)(k-1)+t} \quad (t=1, \dots, \kappa-1; k=1, \dots, r)$$

uniquely determine $\lambda_{i1}, \dots, \lambda_{i, (\kappa-1)r}$ as linear functions of the remaining λ_{ij} , since the determinant of the coefficients of the former equals $|\bar{B}|$. Let (λ) denote the matrix in (98) and

$$(104) \quad L = (\lambda_{ij}) \quad [i=1, \dots, \mu; j=(\kappa-1)r+1, \dots, \mu].$$

We have the following relation between matrices of order μ :

$$(105) \quad (\lambda)(\widetilde{B\Omega}) = (\widetilde{B'L}),$$

where Ω is a matrix of μ rows and $\mu - (\kappa - 1)r$ columns, all of whose elements are zero, except those lying in the main diagonal of $\widetilde{B\Omega}$ which equal unity, i. e.,

$$(106) \quad \Omega = (\delta_{i, (\kappa-1)r+j}) \quad [i=1, \dots, \mu; j=1, \dots, \mu - (\kappa-1)r].$$

Hence by (103) and (105),

$$(107) \quad B' = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ . & . & . & . \\ 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ . & . & . & . \end{bmatrix}, \quad |\widetilde{B'L}| = |\lambda_{ij}| \quad [i, j = (\kappa-1)r+1, \dots, \mu].$$

Hence, by (105), if we take the last determinant different from zero, we have $|\lambda| \neq 0$ in (98).

We assume that this preliminary normalization has been made, so that in L_i matrix B has the form (107₁). Let

$$(108) \quad A_i = (\alpha_{ij}), \quad \bar{A} = \left. \begin{matrix} A_1 \\ \vdots \\ A_r \end{matrix} \right\} [t=1, \dots, \kappa-1; j=1, \dots, (\kappa-1)r],$$

so that A_i is composed of the first $(\kappa-1)r$ columns of A_i . Then $\bar{A} = \bar{A}B = AB$, so that $\bar{A} = M$, where M is the matrix displayed in (59). Set

$$(109) \quad a_i = (\kappa-1)(i-1) \quad (i=1, \dots, r).$$

Then the final equations in (50) may be replaced by

$$\delta \xi_{3\kappa r + a_i + t} = -\tau_{it} \quad (i=1, \dots, r).$$

In (51) the terms of the sum given by $j=1, \dots, (\kappa-1)r$ reduce to

$$\frac{1}{4} (\xi_{3\kappa r + a_i + t-1} + 2\xi_{3\kappa r + a_i + t} + \xi_{3\kappa r + a_i + t+1}),$$

subject to the restrictions noted on (113). Apply the transformation of variables

$$(110) \quad \eta_{3\kappa r + i} = \xi_{3\kappa r + i} + \sum_{j=(\kappa-1)r+1}^{\mu} \lambda_{ij} \xi_{3\kappa r + j} \quad [i=1, \dots, (\kappa-1)r],$$

from which $\xi = \eta - \sum \lambda \eta$. Then L_i is altered in form and

$$\tau_{it}(\xi) = \tau_{it}(\eta) - \frac{1}{4} \sum_{j=(\kappa-1)r+1}^{\mu} \alpha'_{itj} \eta_{3\kappa r + j},$$

$$\alpha'_{itj} \equiv \lambda_{a_i + t-1, j} + 2\lambda_{a_i + t, j} + \lambda_{a_i + t+1, j}.$$

Hence $(\alpha') = M(\lambda_{ij})$, where (λ_{ij}) is the matrix in (110). Taking $(\lambda) = M^{-1}(\alpha)$, we have $(\alpha') = (\alpha)$. Hence the effect of this normalization is to set $\alpha_{ij} = 0$ for $j > (\kappa-1)r$. Finally, we replace

$$(111) \quad \xi_{3\kappa r + a_i + t} \text{ by } \xi_{3\kappa r + (t-1)r + i} \quad (i=1, \dots, r; t=1, \dots, \kappa-1),$$

noting that $a_i + t = a_k + t'$ implies $i = k, t = t'$. Hence

$$(112) \quad L_i: \text{first four equations as in (50), } \delta \xi_{3(\kappa+t-1)r+i} = -\tau_{it} \quad (i=1, \dots, r),$$

where τ_{it} is given by (51) with the final sum replaced by

$$(113) \quad \frac{1}{4} (\xi_{3(\kappa+t-2)r+i} + 2\xi_{3(\kappa+t-1)r+i} + \xi_{3(\kappa+t)r+i}),$$

the first term being absent if $t=1$, the third if $t=\kappa-1$. We have now proved, for $q=4\kappa$, the following

THEOREM. *For any field F having neither modulus 2 nor a modulus which divides q , all linear homogeneous groups in F , which are simply isomorphic with the symmetric group on q letters and which satisfy the condition*

$s = 0$ imposed in § 11, are equivalent under linear transformation in F to a direct product of r linear groups, with fixed coefficients cogredient in the r sets of variables

$$(114) \quad \xi_i, \xi_{r+i}, \xi_{2r+i}, \dots, \xi_{(q-2)r+i} \quad (i=1, \dots, r).$$

To prove the theorem for the remaining cases, we normalize T_κ and $T_{\kappa+1}$ simultaneously with the L_t .

First, let $q = 4\kappa + 1$. For T_κ , given by (66), we have (99) with $t = \kappa$. The above proof is to be modified by changing $\kappa - 1$ to κ , allowing t to take the additional value κ , and by taking as M the matrix defined at the end of § 14. We find that L_t is given by (112), with no suppression in τ_{ii} when $t = \kappa - 1$, and that

$$(115) \quad T_\kappa: \delta\xi_{(3\kappa-2)r+i} = \delta\xi_{(3\kappa-1)r+i} = \tau_{i\kappa}, \quad \delta\xi_{(4\kappa-1)r+i} = -\tau_{i\kappa} \quad (i=1, \dots, r),$$

$$(116) \quad \tau_{i\kappa} = -\frac{1}{2}\xi_{(3\kappa-2)r+i} - \frac{1}{4}\xi_{(3\kappa-1)r+i} + \frac{1}{4}\xi_{(4\kappa-2)r+i} + \frac{5}{4}\xi_{(4\kappa-1)r+i}.$$

For $q = 4\kappa + 2$, we apply transformation (99) with $i, j = r+1, \dots, \mu$, and modify the proof in the light of § 15. In particular, $t = 1, \dots, \kappa$, and $j > r$ in (100), (101). Hence

$$(117) \quad L_t: \text{first four equations as in (50)}, \quad \delta\xi_{(3\kappa+t)r+i} = -\tau_{ii} \quad (i=1, \dots, r),$$

where τ_{ii} is given by (51) with the final sum replaced by

$$(118) \quad \frac{1}{4}(\xi_{(3\kappa+t-1)r+i} + 2\xi_{(3\kappa+t)r+i} + \xi_{(3\kappa+t+1)r+i}),$$

the first term being absent if $t = 1$. Furthermore,

$$(119) \quad T_\kappa: \text{first three equations as in (66')}, \quad \delta\xi_{4\kappa r+i} = -\tau_{i\kappa} \quad (i=1, \dots, r),$$

$$(120) \quad \tau_{i\kappa} = -\frac{1}{2}\xi_{(3\kappa-2)r+i} - \frac{1}{4}\xi_{(3\kappa-1)r+i} + \frac{1}{2}\xi_{3\kappa r+i} + \frac{1}{4}\xi_{(4\kappa-1)r+i} + \frac{3}{4}\xi_{4\kappa r+i}.$$

Finally, for $q = 4\kappa + 3$, the proof is quite similar to that in the preceding case. Here t takes the further value $\kappa + 1$. We obtain the same normalized forms for L_τ and T_κ , except that now

$$(121) \quad \tau_{i\kappa} = \frac{1}{2}\xi_{(4\kappa+1)r+i} + \text{the five terms of (120)}.$$

Furthermore,

$$(122) \quad T_{\kappa+1}: \delta\xi_{3\kappa r+i} = \tau_{i\kappa+1}, \quad \delta\xi_{(4\kappa+1)r+i} = -\tau_{i\kappa+1} \quad (i=1, \dots, r),$$

$$(123) \quad \tau_{i\kappa+1} = -\frac{1}{2}\xi_{3\kappa r+i} + \frac{1}{2}\xi_{4\kappa r+i} + \frac{3}{2}\xi_{(4\kappa+1)r+i}.$$

23. Since the linear groups exhibited in § 22 are direct products of r similar groups, it suffices to know the character of the component groups. We shall list the quadratic invariants of the groups for the case $r = 1$, assuming still that the field has neither modulus 2, nor a modulus dividing q . Set

$$(124) \quad f = \xi_1^2 + \xi_2^2 + \frac{1}{2}\xi_3^2 + \xi_4^2 + \xi_5^2 + \frac{1}{2}\xi_6^2 + \dots + \xi_{3\kappa-2}^2 + \xi_{3\kappa-1}^2 + \frac{1}{2}\xi_{3\kappa}^2.$$

Then the only quadratic invariant of the group is

$$(125) \quad f + \xi_{3\kappa+1}^2 + \xi_{3\kappa+1} \xi_{3\kappa+2} + \xi_{3\kappa+2}^2 + \xi_{3\kappa+2} \xi_{3\kappa+3} + \xi_{3\kappa+3}^2 + \cdots \quad (q = 4\kappa),$$

$$+ \xi_{4\kappa-2}^2 + \xi_{4\kappa-2} \xi_{4\kappa-1} + \xi_{4\kappa-1}^2$$

$$(126) \quad \text{terms of (125)} + \xi_{4\kappa-1} \xi_{4\kappa} + \frac{5}{2} \xi_{4\kappa}^2 \quad (q = 4\kappa + 1),$$

$$(127) \quad f + \xi_{3\kappa+1}^2 + \xi_{3\kappa+2}^2 + \xi_{3\kappa+2} \xi_{3\kappa+3} + \xi_{3\kappa+3}^2 + \cdots \quad (q = 4\kappa + 2),$$

$$+ \xi_{4\kappa-1}^2 + \xi_{4\kappa-1} \xi_{4\kappa} + \xi_{4\kappa}^2 + \xi_{4\kappa} \xi_{4\kappa+1} + \frac{3}{2} \xi_{4\kappa+1}^2$$

$$(128) \quad \text{terms of (127)} + 2\xi_{4\kappa+1} \xi_{4\kappa+2} + 3\xi_{4\kappa+2}^2 \quad (q = 4\kappa + 3).$$

The discriminant of the quadratic invariant is $2^l |P|$, where $l = 2\kappa$ in the first two cases and $l = 2\kappa + 1$ in the last two; while, for $q = 4\kappa$, P is the matrix (57) of order $\kappa - 1$; for $q = 4\kappa + 1$ and $4\kappa + 2$, P is the matrix of order κ defined at the end of §§ 14 and 15; and for $q = 4\kappa + 3$, P is the matrix (96) of order $\kappa + 1$. The matrix of the discriminant therefore reflects an essential property of the group. In each case the discriminant is not zero.

24. In conclusion, we consider briefly the normalization of our linear groups for the case of fields having a modulus p ($p > 2$) which divides q . It is no longer true that, for a given value of r , the groups are all equivalent under linear transformation. For simplicity, we consider only the case in which the number of variables is the minimum $(q - 2)r$.

Let first $q = 4\kappa$. Then by hypothesis $\mu = (\kappa - 2)r$, and the modulus divides κ . Matrices A^* and B^* , defined at the end of § 13, are now square matrices of order $\mu = (\kappa - 2)r$, and each has its determinant $\neq 0$ by (59*). Hence in (98) and (99) we may take $(\lambda_{ij}) = (B^*)^{-1}$. After this normalization, we have $B^* = I$. Now by (59),

$$AB^* = N = \begin{pmatrix} P'O \cdots O \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ OO \cdots P' \end{pmatrix},$$

where P' is derived from P , given by (57), by deleting the last column. Hence $A = N$. The $\beta_{jk\kappa-1}$ are now uniquely determined by (59). Set

$$\beta_{(\kappa-2)(i-1)+v, k, \kappa-1} = b_v \quad (i, k = 1, \cdots, r; v = 1, \cdots, \kappa - 2).$$

Then

$$2b_1 + b_2 = 0, \quad b_1 + 2b_2 + b_3 = 0, \cdots, \quad b_{v-1} + 2b_v + b_{v+1} = 0, \cdots,$$

$$b_{\kappa-3} + 2b_{\kappa-2} = \delta_{ik}, \quad b_{\kappa-2} = 2\delta_{ik}.$$

Since the eliminant of these $\kappa - 1$ equations is $|P|$, a multiple of the modulus, there is a unique set of solutions:

$$b_v = (-1)^{\kappa-v} (\kappa - v) \delta_{ik}.$$

Proceeding similarly when $q = 4\kappa + 1, \dots, 4\kappa + 3$, we obtain the

THEOREM. *When the field F has a modulus p ($p > 2$) which divides q , all linear homogeneous groups, which are simply isomorphic with the symmetric groups on q letters, and which affect the minimum number $(q - 2)r$ of variables under the hypothesis of § 11, are equivalent under linear transformation in F to a direct product of r cogredient linear groups with fixed coefficients.*

It is sufficient to exhibit one of the component groups. Hence we set $r = 1$.

For $q = 4\kappa$, $L_i(t \leq \kappa - 2)$ is defined by (112) for $r = i = 1$, with the first term of (113) deleted if $t = 1$, and the last term if $t = \kappa - 2$. Also

$$(129) \quad L_{\kappa-1}: \delta\xi_{3\kappa-4} = \delta\xi_{3\kappa-3} = \tau_{\kappa-1}, \quad \delta\xi_{3\kappa-2} = \delta\xi_{3\kappa} = -\tau_{\kappa-1}, \quad \delta\xi_{3\kappa+j} = (-1)^{\kappa-j} j \tau_{\kappa-1} \\ (j = 1, \dots, \kappa - 2),$$

$$(130) \quad \tau_{\kappa-1} = -\frac{1}{2}\xi_{3\kappa-4} - \frac{1}{4}\xi_{3\kappa-3} + \frac{1}{2}\xi_{3\kappa-2} + \frac{1}{4}\xi_{3\kappa} + \frac{1}{4}\xi_{4\kappa-2}.$$

For $q = 4\kappa + 1$, L_i is given by (112) for $r = i = 1$, with the suppressions noted on (113), while

$$(131) \quad T_{\kappa}: \delta\xi_{3\kappa-1} = \delta\xi_{3\kappa} = \tau_{\kappa}, \quad \delta\xi_{3\kappa+j} = -(-1)^{\kappa-j} 4j \tau_{\kappa} \quad (j = 1, \dots, \kappa - 1),$$

$$(132) \quad \tau_{\kappa} = -\frac{1}{2}\xi_{3\kappa-1} - \frac{1}{4}\xi_{3\kappa} + \frac{1}{4}\xi_{4\kappa-1}.$$

For $q = 4\kappa + 2$, L_i is given by (117) for $r = i = 1$, with the first term of (118) suppressed if $t = 1$, and the last term if $t = \kappa - 1$. Also

$$(133) \quad T_{\kappa}: \delta\xi_{3\kappa-1} = \delta\xi_{3\kappa} = \tau_{\kappa}, \quad \delta\xi_{3\kappa+1} = -\tau_{\kappa}, \quad \delta\xi_{3\kappa+j} = (-1)^{\kappa-j} (2j - 2) \tau_{\kappa} \quad (j = 2, \dots, \kappa),$$

$$(134) \quad \tau_{\kappa} = -\frac{1}{2}\xi_{3\kappa-1} - \frac{1}{4}\xi_{3\kappa} + \frac{1}{2}\xi_{3\kappa+1} + \frac{1}{4}\xi_{4\kappa}.$$

Finally, for $q = 4\kappa + 3$, L_i is given by (117), with the first term of (118) suppressed if $t = 1$; T_{κ} is given by (119), while

$$(135) \quad T_{\kappa+1}: \delta\xi_{3\kappa+1} = \tau_{\kappa+1}, \quad \delta\xi_{2\kappa+j} = -(-1)^{\kappa-j} (4j - 4) \tau_{\kappa+1} \quad (j = 2, \dots, \kappa + 1),$$

$$(136) \quad \tau_{\kappa+1} = -\frac{1}{2}\xi_{3\kappa+1} + \frac{1}{2}\xi_{4\kappa+1}.$$

We may now show that in the present case for which the modulus divides q , the quadratic invariant of the group is obtained from the invariant when the modulus is prime to q by suppressing the final two terms. For instance, if $q = 4\kappa + 1$ the invariant is (125), if $q = 4\kappa + 3$ the invariant is (127).